
Besonders schützenswerte Personendaten

Zu den Anforderungen an die Rechtmässigkeit der Bearbeitung durch öffentliche Organe im Falle des Fehlens einer gesetzlichen Grundlage

ASTRID EPINEY

Dieser Beitrag wurde erstmals wie folgt veröffentlicht:

Astrid Epiney, Besonders schützenswerte Personendaten – Zu den Anforderungen an die Rechtmässigkeit der Bearbeitung durch öffentliche Organe im Falle des Fehlens einer gesetzlichen Grundlage, FS Paul-Henri Steinauer, Bern 2013, 97-112. Es ist möglich, dass die Druckversion – die allein zitierfähig ist – im Verhältnis zu diesem Manuskript geringfügige Modifikationen enthält.

Inhaltsverzeichnis

I.	Einleitung.....	1
II.	Zum Konzept der besonders schützenswerten Personendaten.....	2
III.	Ausgewählte Surrogate einer Rechtsgrundlage – Versuch einer Auslegeordnung.....	5
	1. Zur Einwilligung	6
	2. Zwingende Notwendigkeit zur Erfüllung einer gesetzlichen Aufgabe	9
IV.	Schlussbemerkung	13
	Literatur	15

I. Einleitung

Bestimmte Kategorien von Daten werden im Datenschutzrecht aufgrund ihrer (vermuteten) Sensitivität und damit des erhöhten Risikopotentials ihrer Bearbeitung für die Persönlichkeitsrechte der Betroffenen einem besonderen Schutz unterstellt. Dieser besondere Schutz kann sich auf verschiedene Aspekte beziehen (z.B. die Reichweite der Informationspflichten Rechtfertigungsgründe einer Bearbeitung). Soweit die Datenbearbeitung durch öffentliche Organe betroffen ist, kommt in diesem Zusammenhang dem grundsätzlichen Erfordernis des Bestehens einer gesetzlichen Grundlage für die Datenbearbeitung – das allgemein, also auch für nicht besonders schützenswerte

Personendaten, gilt – und den hiervon vorgesehenen Ausnahmen eine besondere Bedeutung zu.

So dürfen besonders schützenswerte Personendaten sowie Persönlichkeitsprofile nach Art. 17 Abs. 2 DSG grundsätzlich nur bearbeitet werden, wenn ein Gesetz im formellen Sinn es ausdrücklich vorsieht. „Ausnahmsweise“ ist eine Bearbeitung solcher Daten nach dieser Bestimmung auch zulässig, wenn (u.a.) diese für eine in einem Gesetz im formellen Sinn klar umschriebene Aufgabe „unentbehrlich“ ist oder die betroffene Person im Einzelfall eingewilligt hat. Die kantonalen Datenschutzgesetze enthalten in der Regel ähnliche Bestimmungen.¹

Aufgeworfen wird damit die Frage, welche Anforderungen genau im Falle des möglichen Greifens dieser Ausnahmen vom grundsätzlichen Erfordernis einer gesetzlichen Grundlage zu beachten sind bzw. wie diese Bestimmungen auszulegen sind, eine Frage, die auch und gerade im Zusammenhang mit elektronisch betriebenen Informationssystemen von grosser Bedeutung ist. Im Folgenden soll dieser Problematik nachgegangen werden (III.), dies auf der Grundlage einer Skizzierung des Konzepts der besonders schützenswerten Personendaten (II.). Der Beitrag schliesst mit einer kurzen Schlussbemerkung (IV.).²

II. Zum Konzept der besonders schützenswerten Personendaten

Die Grundidee „besonders schützenswerter Personendaten“ ist vor dem Hintergrund zu sehen, dass bestimmte Kategorien von Personendaten bzw. ihre Bearbeitung deshalb einen erhöhten Schutz verdienen, weil mit der entsprechenden Bearbeitung ein besonderes Risiko für die Persönlichkeitsrechte der Betroffenen einhergeht. Deutlich wird damit, dass bei der Identifizierung derjenigen Personendaten, die als besonders schützenswert angesehen werden, zwei grundsätzliche Herangehensweisen denkbar sind (die aber auch miteinander kombiniert werden können):³

¹ Vgl. die Nachweise bei WALDMANN/OESCHGER, in: Belser/Epiney/Waldmann, Datenschutzrecht, § 13, N 42.

² Auch der Jubilar befasste sich in verschiedener Hinsicht eingehend mit dem Datenschutzrecht. Zu erwähnen ist insbesondere seine langjährige Mitgliedschaft in der Eidgenössischen Datenschutzkommission. Vgl. in diesem Zusammenhang STEINAUER, ZBl. 2007, 354 ff. Ihm sei dieser Beitrag in grosser Dankbarkeit für die sehr angenehme Zusammenarbeit und die vielfältige Unterstützung gewidmet.

³ Hierzu z.B. TERWANGNE, in: Die Entwicklung der europarechtlichen Vorgaben im Bereich des Datenschutzes, 23 (42 ff.); s. auch schon EPINEY/HOFSTÖTTER/MEIER/THEUERKAUF, Schweizerisches Datenschutzrecht vor europa- und völkerrechtlichen Herausforderungen, 23 ff.

- Erstens ist es möglich, Angaben über bestimmte persönliche Merkmale, Ansichten oder den Werdegang als besonders schützenswert einzustufen. Dieser Ansatz ist heute in der Schweiz vorherrschend. So definiert Art. 3 lit. c DSG als besonders schützenswert diejenigen Personendaten, die die religiösen, weltanschaulichen, politischen oder gewerkschaftlichen Ansichten oder Tätigkeiten, die Gesundheit, die Intimsphäre oder die Rassenzugehörigkeit, Massnahmen der sozialen Hilfe oder administrative oder strafrechtliche Verfolgungen und Sanktionen betreffen. Die kantonalen Datenschutzgesetze enthalten grösstenteils ähnliche Definitionen.⁴
- Zweitens kann auf die konkrete Art der Datenbearbeitung abgestellt werden, so dass diejenigen Personendaten als besonders schützenswert angesehen werden, bei denen wegen ihrer Bedeutung, des Kontexts, des Zwecks oder der Art ihrer Bearbeitung eine besonders grosse Gefahr der Persönlichkeitsverletzung besteht. Dieser Ansatz wird in der Schweiz im Kanton Aargau zugrundegelegt, während der Kanton Zürich auf ihn in Kombination mit einer katalogartigen Aufzählung zurückgreift.⁵

Die Datenschutzkonvention des Europarates (DSK)⁶ legt – ebenso wie die EU-Datenschutzrichtlinie⁷ – derzeit ebenfalls den erstgenannten Ansatz zugrunde (Art. 6 DSK). Vor dem Hintergrund, dass nicht nur die Zuordnung von Personendaten zu einer bestimmten Kategorie etwas über die (bei den besonders schützenswerten Daten im Vordergrund stehende) Frage nach dem Ausmass der (potentiellen) Gefährdung der Persönlichkeitsrechte der Betroffenen aussagt,⁸ soll dieser Ansatz im Rahmen der derzeit laufenden Revision der Datenschutzkonvention des Europarates⁹ aber zugunsten eines kombinierten Ansatzes aufgegeben werden. Der derzeit vorliegende Vorschlag stellt auf die Gefahr eines grossen Risikos für die Interessen und Rechte der Betroffenen (insbesondere diejenige einer Diskriminierung) durch die entsprechende Datenbearbeitung ab. Eine solche Gefahr wird bei bestimmten Datenkategorien (genetische Daten, Gesundheitsdaten sowie Angaben über das Sexualleben, strafrechtliche Vergehen oder Verbrechen sowie diesbezügliche Urteile oder Massnahmen) als gegeben angesehen; bei anderen Datenkategorien ist hierfür erforderlich, dass die Daten gerade wegen ihres entspre-

⁴ Vgl. die Nachweise bei WALDMANN/OESCHGER, in: Belser/Epiney/Waldmann, Datenschutzrecht, § 13, N 21.

⁵ Vgl. die Nachweise bei WALDMANN/OESCHGER, in: Belser/Epiney/Waldmann, Datenschutzrecht, § 13, N 21.

⁶ Konvention Nr. 108 zum Schutz des Einzelnen im Hinblick auf die automatische Verarbeitung personenbezogener Daten, SR 0.235.1.

⁷ RL 95/46 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. 1995 L 281, 31.

⁸ Zur Problematik der „sensitiven“ Daten und der verschiedenen Ansätze schon EPINEY/HOFSTÖTTER/MEIER/THEUERKAUF, Schweizerisches Datenschutzrecht vor europä- und völkerrechtlichen Herausforderungen, 23 ff.

⁹ Zu dieser Revision z.B. TERWANGNE, in: Die Entwicklung der europarechtlichen Vorgaben im Bereich des Datenschutzes, 23 ff.; FASNACHT, SJER 2011/2012, 329 ff.

chenden Inhalts bearbeitet werden (dies betrifft Angaben über die Rasse, die politische Meinung, die Gewerkschaftszugehörigkeit, die religiösen oder sonstigen Überzeugungen sowie biometrische Daten).¹⁰ Die Schweiz müsste die entsprechenden Definitionen im Bundesrecht und in den meisten kantonalen Datenschutzgesetzen im Falle der Modifikation der Konvention (und ihrer Ratifikation, welche zu erwarten ist) anpassen.¹¹

Jedenfalls ist – auf der Grundlage beider Ansätze – davon auszugehen, dass zahlreiche Datenbearbeitungen durch öffentliche Organe (sei dies nun auf Bundesebene oder auf kantonaler Ebene) besonders schützenswerte Personendaten betreffen. Während hierfür auf Bundesebene in aller Regel eine formell-gesetzliche Grundlage im Sinn des Art. 17 Abs. 2 DSG gegeben ist, dürfte dies in den Kantonen häufig nicht der Fall sein. Dies wird etwa relevant, wenn in den Kantonen bzw. Gemeinden Daten über sozialhilfeabhängige Personen oder über Personen, in Bezug welche fürsorgerische oder vormundschaftliche Massnahmen ergriffen werden, bearbeitet werden. Dabei ist davon auszugehen, dass derartige Bearbeitungen heute meist mittels computerisierter Informationssysteme, auf die mehrere, oft zahlreiche Personen (teilweise) Zugriff haben, erfolgen. Deutlich wird damit die Relevanz der datenschutzrechtlichen Anforderungen, die in Bezug auf derartige Datenbearbeitungen zum Zuge kommen.

Dabei sei in diesem Zusammenhang auch darauf hingewiesen, dass sich die erhöhten Anforderungen an die Rechtmässigkeit der Bearbeitung besonders schützenswerter Personendaten und damit die rechtliche Grundlage (bzw. die zulässigen Ausnahmen von derselben) im Ansatz bereits aus Art. 8 EMRK ergeben: So geht der Gerichtshof für Menschenrechte in ständiger Rechtsprechung davon aus, dass für bestimmte Kategorien von Eingriffen in Art. 8 EMRK unterschiedlich weitgehende Vorgaben an die Qualität der gesetzlichen Grundlage zum Zuge kommen, so dass für besonders Gruppen von (angesichts der Reichweite der möglichen Persönlichkeitsbeeinträchtigung bzw. der Beeinträchtigung der Privatsphäre) eher schweren Eingriffen erhöhte Anforderungen gestellt werden.¹²

Im Übrigen ergibt sich auch bereits aus dem Gesetzmässigkeitsprinzip, dass die Anforderungen an die Präzision und Form der gesetzlichen Grundlage mit der Intensität der Datenbearbeitungen bzw. mit dem Risikopotenzial für allfällige Persönlichkeitsverletzungen steigen. Sobald also in einem gewissen Umfang und mit einer gewissen „Verbreitung“ (was die Zugangsberechtigten angeht) besonders schützenswerte Daten bearbeitet werden, ist die gesetzliche Grundlage sehr genau zu fassen, und grundsätzlich ist eine for-

¹⁰ Vgl. ausführlich zu diesem Vorschlag TERWANGNE, in: Die Entwicklung der europarechtlichen Vorgaben im Bereich des Datenschutzes, 23 (44 ff.).

¹¹ Hierzu FASNACHT, SJER 2011/2012, 329 (343 ff.).

¹² Vgl. zur Rechtsprechung des EGMR zu dieser Problematik, m.w.N., EPINEY/SCHLEISS, in: Belser/Epiney/Waldmann, Datenschutzrecht, § 13, N 17.

mell-gesetzliche Grundlage notwendig. In diesem Sinn formuliert auch Art. 36 Abs. 1 S. 2, dass schwerwiegende Einschränkungen von Grundrechten im Gesetz selbst (also in einer formell-gesetzlichen Grundlage) vorgesehen sein müssen, eine Vorgabe, die auch für die kantonale Ebene von Bedeutung ist.¹³ Dies schliesst Surrogate einer solchen ausdrücklichen gesetzlichen Grundlage nicht von vornherein aus, setzt ihrer Ausgestaltung jedoch gewisse (wohl eher enge) Grenzen.

III. Ausgewählte Surrogate einer Rechtsgrundlage – Versuch einer Auslegeordnung

Sowohl auf Bundesebene als auch auf kantonaler Ebene sind als Surrogate einer (klaren) gesetzlichen Grundlage für die Bearbeitung besonders schützenswerter Personendaten – wie bereits eingangs erwähnt¹⁴ – durchwegs zwei Konstellationen vorgesehen:

- Erstens ist eine solche Bearbeitung zulässig, wenn sie zur Erfüllung einer gesetzlich vorgesehenen Aufgabe „zwingend“, „unbedingt erforderlich“¹⁵ oder „unentbehrlich“ (so Art. 17 Abs. 2 lit. a DSG) ist.
- Zweitens vermag eine Einwilligung auch eine Bearbeitung besonders schützenswerter Personendaten rechtfertigen, wenn auch hierfür ggf. erhöhte Anforderungen zum Zuge kommen, so dass die Einwilligung z.B. nur „im Einzelfall“ (vgl. Art. 17 Abs. 2 lit. c DSG) möglich ist oder / und „ausdrücklich“¹⁶ zu erfolgen hat.

Im Folgenden sollen die genauen Anforderungen, die im Rahmen dieser Surrogate einer Rechtsgrundlage zum Zuge kommen, einer gewissen Präzisierung zugeführt werden. Dabei ist davon auszugehen, dass die Voraussetzungen für das Greifen der erwähnten Surrogate für eine gesetzliche Grundlage im Falle der Bearbeitung besonders schützenswerter Personendaten grundsätzlich so auszulegen sind, dass im Verhältnis zur Bearbeitung „normaler“ Personendaten strengere Anforderungen zum Zuge kommen, impliziert die Bearbeitung besonders schützenswerter Personendaten doch grundsätzlich einen schwereren Eingriff in die Persönlichkeitsrechte der Betroffenen. Vor diesem Hintergrund kommt ein

¹³ Vgl. zur Rechtsprechung des EGMR zu dieser Problematik, m.w.N., EPINEY/SCHLEISS, in: Belser/Epiney/Waldmann, Datenschutzrecht, § 13, N 17; zu den verfassungsrechtlichen Vorgaben BELSER, in: Belser/Epiney/Waldmann, Datenschutzrecht, § 6, N 6 ff.; s. auch WALDMANN/BICKEL, in: Belser/Epiney/Waldmann, Datenschutzrecht, § 12, N 51.

¹⁴ Oben I.

¹⁵ Vgl. die Nachweise für die Formulierungen in den kantonalen Datenschutzgesetzen bei WALDMANN/OESCHGER, in: Belser/Epiney/Waldmann, Datenschutzrecht, § 13, N 42.

¹⁶ So Art. 4 Abs. 5 S. 2 DSG sowie in der Regel die kantonalen Gesetze, vgl. die Nachweise für die kantonale Gesetzgebung bei WALDMANN/OESCHGER, in: Belser/Epiney/Waldmann, Datenschutzrecht, § 13, N 43 ff.

Verzicht auf eine gesetzliche Grundlage vor dem Hintergrund der der Verfassung und der EMRK zu entnehmenden Vorgaben¹⁷ grundsätzlich nur in engen Grenzen in Betracht.

1. Zur Einwilligung

Eine Einwilligung vermag eine Datenbearbeitung von vornherein nur dann zu rechtfertigen, wenn sie in Kenntnis aller Umstände freiwillig und zweifelsfrei sowie (bei besonders schützenswerten Daten) „ausdrücklich“ (so Art. 4 Abs. 5 S. 2 DSGVO) erfolgt.¹⁸ Im Einzelnen sind hier in erster Linie folgende Elemente von Bedeutung:

- Eine Einwilligung ist nur auf der Grundlage einer angemessenen Information gültig.¹⁹ Diese muss sich daher auf alle Umstände beziehen, die für die Einwilligung in die Datenbearbeitung von Bedeutung sind. In der Regel impliziert dies mindestens eine Information über Art und Umfang der Datenbearbeitung, die Datenbearbeiter, den Zweck der Datenbearbeitung sowie ggf. ihre Risiken. Der genaue Umfang der Informationspflicht kann aber nur im Einzelfall unter Berücksichtigung aller Umstände bestimmt werden. Leitmotiv muss jedenfalls sein, dass die Information es ermöglicht, die Tragweite der Einwilligung zu erkennen. Dies impliziert auch, dass die Art und Weise der Information für die Betroffenen verständlich sein muss; Irreführungen oder versteckte Hinweise sind zu vermeiden.²⁰ Welche Form die Information annehmen muss, ist auch vor dem Hintergrund des Sinns und Zwecks der Informationspflicht nach den Umständen des Einzelfalls zu entscheiden.²¹ Grundsätzlich ungenügend ist eine nachträgliche Information, da sie keine angemessene Information zum Zeitpunkt der Einwilligung zu begründen vermag, wobei allerdings eine nachträgliche Einwilligung in eine Datenbearbeitung ebenfalls möglich sein kann.²²

¹⁷ Zu diesen die Hinweise oben II.

¹⁸ Vgl. zur Einwilligung allgemein, m.w.N., MEIER, Protection des données, § 4, N 823 ff.; EPINEY, in: Belser/Epiney/Waldmann, Datenschutzrecht, § 9, N 15 ff.

¹⁹ Vgl. für die Bundesebene Art. 4 Abs. 5 S. 1 DSGVO; zu den entsprechenden kantonalen Bestimmungen WALDMANN/OESCHGER, in: Belser/Epiney/Waldmann, Datenschutzrecht, § 13, N 43 ff.

²⁰ HÄNER, ZBl. 2002 57 (64), weist zutreffend darauf hin, dass die einwilligende Person den gleichen Wissensstand haben muss wie im Falle des Bestehens einer Rechtsgrundlage für die Bearbeitung.

²¹ ROSENTHAL, in: Rosenthal/Jöhri, Handkommentar DSGVO, Art. 4, N 75. Vgl. für ein Beispiel die Ausführungen in BVGer, Urt. A-3908/2008, 2009/44, Urt. v. 4.8.2009, E. 4.4, in Bezug auf die Anforderungen an die Information bei der Bekanntgabe biometrischer Daten (Fingerabdruck) im Hinblick auf die Eingangskontrolle in einem Schwimmbad. S. auch die Präzisierungen bei MEIER, Protection des données, § 4, N 860 ff.

²² Vgl. WERMELINGER/SCHWERI, Jusletter v. 3.3.2008, N 12.

- Freiwillig ist die Einwilligung immer dann, wenn sie ohne Druck zustande gekommen ist, wobei ein solcher wohl nur dann anzunehmen ist, wenn der mit der Verweigerung der Einwilligung zu der Datenbearbeitung verbundene Nachteil in keinem Zusammenhang mit der Datenbearbeitung und der mit ihr verfolgten Zielsetzung steht oder unverhältnismässig ist, so dass nicht jeder mit der Verweigerung der Datenbearbeitung verbundene Nachteil die Freiwilligkeit ausschliesst²³.
- Bei besonders schützenswerten Daten muss die Einwilligung zudem ausdrücklich erfolgen. Ausdrücklich ist eine Einwilligung wohl immer erst dann, wenn sowohl ihr Inhalt (also der Bezug zu einer bestimmten, ggf. näher präzisierten Datenbearbeitung, so dass die Einwilligung klar sein muss) als auch die Form ausdrücklich (so dass eine konkludente Einwilligung nicht ausreichend sein dürfte) erfolgt bzw. ist, so dass jedenfalls eine klare Einverständniserklärung (die aber nicht unbedingt schriftlich sein muss, wobei der Datenbearbeitende jedoch die Beweislast trägt) zu verlangen ist.²⁴
- Fraglich könnte noch sein, ob eine Einwilligung bei besonders schützenswerten Personendaten immer nur im Einzelfall eine Datenbearbeitung zu rechtfertigen vermag, wie dies in Art. 17 Abs. 2 lit c DSG für die Bundesebene formuliert ist. Im Ergebnis dürfte diese Frage – immer für den Fall, dass das einschlägige kantonale Gesetz keine solche Anforderung kennt – zu verneinen sein: Denn obwohl die Bearbeitung besonders schützenswerter Personendaten grundsätzlich einen eher weitgehenden Eingriff in die Persönlichkeitsrechte der Betroffenen impliziert, mag es doch Fallgestaltungen geben, in denen die Schwere des Eingriffs in einer konkreten

²³ BBl 2003 2127, mit einigen Beispielen. Weitere Beispiele bei ROSENTHAL, in: Rosenthal/Jöhri, Handkommentar DSG, Art. 4, N 97 f. S. auch WERMELINGER/SCHWERI, Jusletter v. 3.3.2008, N 11, die davon sprechen, dass letztlich ähnliche Anforderungen zum Zuge kommen wie bei der Einwilligung in einen chirurgischen Eingriff. Vgl. in diesem Zusammenhang auch die Zusammenfassung der für medizinische Eingriffe geltenden Grundsätze bei MEIER, Protection des données, § 4, N 847 ff.

²⁴ A.A. aber, unter Hinweis auf die verschiedenen Sprachfassungen MEIER, Protection des données, § 4, N 897 ff., sowie ROSENTHAL, in: Rosenthal/Jöhri, Handkommentar DSG, Art. 4 N 83 ff., der anführt, dass sich die Ausdrücklichkeit der Einwilligung nur auf den Inhalt, nicht hingegen auf die Art und Weise der Willenserklärung beziehe, was schon deshalb nicht überzeugt, weil auch eine konkludente Einwilligung sich auf eine bestimmte Datenbearbeitung beziehen muss, so dass die Abgrenzung zwischen ausdrücklicher und nicht ausdrücklicher Einwilligung jedenfalls auch auf die Form abstellen dürfte. Allerdings ist zuzugeben, dass eine ausdrückliche Einwilligung auch dann vorliegen kann, wenn sich die Einwilligung eindeutig und ausdrücklich aus einer bestimmten Erklärung ergibt, so dass es selbstredend nicht darum gehen kann, für die ausdrückliche Einwilligung einen bestimmten Wortlaut zu verlangen. Im Übrigen sind das Verhalten des Betroffenen sowie die sonstigen konkreten Umstände jedenfalls umfassend nach Treu und Glauben zu würdigen, und aus reinem Schweigen oder passivem Dulden darf in aller Regel nicht auf eine Einwilligung geschlossen werden (BVGer, A-3144/2008, Urt. v. 27.5.2009, E. 12.1; s. auch WALDMANN/BICKEL, in: Belser/Epiney/Waldmann, Datenschutzrecht, § 12, N 53). Vor diesem Hintergrund sollte die Bedeutung dieses Meinungsstreits nicht überschätzt werden.

Konstellation zu relativieren ist.²⁵ Vor diesem Hintergrund dürfte aus Art. 8 EMRK und Art. 13 Abs. 2 BV kein solch allgemeines Erfordernis abzuleiten sein. Dies schliesst es aber nicht aus, dass Art und Umstände der konkreten Datenbearbeitung ein solches Erfordernis nahelegen können. Jedenfalls fallen die Anforderungen an die Einwilligung umso höher aus, je stärker der Eingriff in die Persönlichkeitsrechte der betroffenen Person ist.²⁶

Diese relativ strengen Anforderungen implizieren, dass bei der Bearbeitung besonders schützenswerter Personendaten durch öffentliche Organe eine Einwilligung in der Regel nicht zum Tragen kommen kann, insbesondere wenn es um in Informationssystemen gespeicherte und elektronisch abrufbare Daten geht: Regelmässig wird schon eine ausreichende Information zu verneinen sein, denn die Betroffenen dürften in den wenigsten Fällen umfassend über die Art der Datenbank, die genau dort enthaltenen Daten sowie die Zugriffsberechtigten informiert sein. Zudem erscheint es in all denjenigen Konstellationen, in denen kontextunabhängig durch die Berechtigten auf die Daten zugegriffen werden kann, grundsätzlich nicht möglich, im Vorfeld „ausdrücklich“ jedem Zugriff zuzustimmen, sind diese Zugriffe doch mitunter nicht vorhersehbar. Eine angemessene Information erscheint also bei Informationssystemen in aller Regel schwierig bis unmöglich, so dass auch eine Zustimmung zu den entsprechenden Datenbearbeitungen nicht möglich ist. Weiter geht es bei einigen Informationssystemen, die besonders schützenswerte Daten enthalten, um Daten von Personen, die sich in einer irgendwie gearteten Notlage befinden, so dass es zweifelhaft sein kann, ob ihre allfällige Einwilligung in eine sie betreffende Datenbearbeitung wirklich aus freiem Willen erfolgt.

Diese Erwägungen ändern selbstverständlich nichts daran, dass das Vorliegen einer Einwilligung jeweils im Einzelfall zu prüfen ist. Sie verdeutlichen aber die geringe Relevanz dieses Rechtfertigungsgrundes im Falle der Bearbeitung besonders schützenswerter Personendaten durch öffentliche Organe. Relevant werden kann dies z.B. bei Informationssystemen, die von im Sozialhilfebereich oder im Kindes- und Erwachsenenschutz tätigen Behörden verwendet werden und die schon wegen der Art der Tätigkeit regelmässig besonders schützenswerte Personendaten enthalten. Hier sind in aller Regel die angeführten Erwägungen einschlägig, so dass eine Einwilligung als Rechtfertigungsgrund für die Datenbearbeitung grundsätzlich ausscheidet.

²⁵ Vgl. oben II. zur Konzeption der besonders schützenswerten Personendaten.

²⁶ WERMELINGER/SCHWERI, Jusletter v. 3.3.2008, Rn. 13; SCHWEIZER, Data Mining, 180 ff.; a.A. bzw. zumindest missverständlich aber WEBER, Datenschutzrecht vor neuen Herausforderungen, 34.

2. **Zwingende Notwendigkeit zur Erfüllung einer gesetzlichen Aufgabe**

Weiter ist eine ohne eine eigentliche gesetzliche Grundlage erfolgende Bearbeitung besonders schützenswerter Personendaten dann zulässig, wenn sie zur Erfüllung einer gesetzlichen Aufgabe „zwingend“ oder „unbedingt“ erforderlich bzw. unentbehrlich ist.²⁷

Offensichtlich ist es also nicht ausreichend, dass die Datenbearbeitung im Hinblick auf die Erfüllung der gesetzlichen Aufgabe hilfreich ist oder dieser (nur) dient, sondern die Erfüllung der gesetzlichen Aufgabe darf ohne die Bearbeitung der besonders schützenswerten Personendaten nicht möglich sein. M.a.W. würde die Erfüllung der Aufgabe ohne die fragliche Datenbearbeitung geradezu vereitelt,²⁸ so dass es nicht ausreichend ist, dass die Datenbearbeitung die Wahrnehmung der gesetzlichen Aufgabe (nur) erleichterte oder effizienter gestaltete.

Diese Anforderung dürfte sich nicht nur auf den Grundsatz der Bearbeitung besonders schützenswerter Personendaten, sondern auch auf die genaue Ausgestaltung derselben (Umfang der Datenbearbeitung, Ausgestaltung des Zugangs u.a.m.) beziehen. Denn nur dieser Ansatz trägt dem Umstand Rechnung, dass bei der Bearbeitung besonders schützenswerter Personendaten offenbar strengere Anforderungen als die allgemein zu beachtenden Vorgaben zum Zuge kommen sollen. Bezöge man das Erfordernis, dass die Bearbeitung der besonders schützenswerten Personendaten zwingend zur Erfüllung einer gesetzlichen Aufgabe notwendig sein muss, nur auf den Grundsatz der Bearbeitung besonders schützenswerter Personendaten, nicht aber auch ihre konkrete Ausgestaltung, wären im Ergebnis im Verhältnis zu dem so wieso bei jeder Datenbearbeitung massgeblichen Verhältnismässigkeitsgrundsatz kaum zusätzliche Anforderungen zu beachten (wird doch der Grundsatz der Bearbeitung bestimmter besonders schützenswerter Personendaten in zahlreichen Fällen zur Erfüllung einer gesetzlichen Aufgabe zwingend notwendig sein). Im Übrigen und vor allem widerspräche es Sinn und Zweck dieser zusätzlichen Anforderung, die zwingende Erforderlichkeit nur auf den Grundsatz, nicht aber die Modalitäten der Datenbearbeitung zu beziehen: Denn diese Anforderung soll offenbar sicherstellen, dass in dieser Konstellation besonders schützenswerte Personendaten nur unter der Voraussetzung bearbeitet werden, dass dies zwingend zur Wahrnehmung einer gesetzlichen Aufgabe notwendig ist, dies im Hinblick auf den verfassungsrechtlich gebotenen Schutz der Persönlichkeit. Unterschiede man nun zwischen Grund-

²⁷ Vgl. III., am Anfang.

²⁸ Vgl. mit Bezug auf die entsprechende Vorschrift im DSG (Art. 17 Abs. 2 lit. a DSG) JÖHRI, in: Rosenthal/Jöhri, Handkommentar DSG, Art. 17, Rn. 77; Botschaft DSG, BBl 1988 II 468; WALDMANN/BICKEL, in: Belser/Epiney/Waldmann, Datenschutzrecht, § 12, N 53; in Bezug auf entsprechende kantonale Regelungen WALDMANN/OESCHGER, in: Belser/Epiney/Waldmann, Datenschutzrecht, § 13, N 42.

satz und Modalitäten, würde diese Zielsetzung unterlaufen, implizierte ein derartiger Ansatz doch, dass gewisse Bearbeitungen erfolgten, die gerade nicht zwingend für die Wahrnehmung der gesetzlichen Aufgabe notwendig sind. Im Ergebnis muss damit die Bearbeitung besonders schützenswerter Personendaten insgesamt „zwingend“ zur Erfüllung der gesetzlichen Aufgabe notwendig sein, wobei lediglich eine Erleichterung ihrer Wahrnehmung durch die betreffende Datenbearbeitung (in der Form und dem Umfang, wie sie vorgesehen ist) nicht ausreichend ist. So dürfen z.B. nur diejenigen Daten bearbeitet werden, die im Hinblick auf die Erfüllung der gesetzlichen Aufgabe tatsächlich zwingend relevant sind, oder das Dossier ist nur solange aufzubewahren, wie dies zur Erfüllung des gesetzlichen Auftrages zwingend notwendig ist.

Deutlich wird damit auch, dass sich diese Anforderung teilweise mit den allgemeinen Grundsätzen der Zweckbindung und der Verhältnismässigkeit überschneiden, ist es doch z.B. auch eine Frage der Verhältnismässigkeit, ob die Bearbeitung einer bestimmten Angabe zur Erfüllung der gesetzlichen Aufgabe (zwingend) erforderlich ist. Im Übrigen dürfte eine Datenbearbeitung von vornherein nur dann zur Erfüllung einer gesetzlichen Aufgabe zwingend erforderlich sein, wenn sie den Anforderungen der Geeignetheit und der Erforderlichkeit (also des mildesten Mittels in Bezug auf die Beeinträchtigung der Persönlichkeitsrechte der Betroffenen) entspricht. Gute Gründe – insbesondere der bereits erwähnte Grundsatz, dass die Bearbeitung besonders schützenswerter Personendaten erhöhten Anforderungen als diejenige „normaler“ Personendaten zu genügen hat sowie der verfassungs- und menschenrechtlich gebotene Schutz dieser Daten – sprechen hier dafür, dass die Anforderungen an den „zwingenden“ Charakter der Datenbearbeitung zur Erfüllung des gesetzlichen Zwecks tendenziell strenger sind als diejenigen der „normalen“ Erforderlichkeit im Rahmen der Verhältnismässigkeitsprüfung. Dieser Grundsatz wird insbesondere in der bereits erwähnten Anforderungen konkretisiert, dass die Datenbearbeitung (inklusive ihrer Modalitäten) für die Erfüllung der gesetzlichen Aufgabe nicht nur nützlich oder hilfreich, sondern zwingend erforderlich sein muss, so dass allein eine erhöhte Effizienz o.ä. gerade nicht ausreichend ist.

Im Übrigen ist es für die Beantwortung der Frage, ob die Datenbearbeitung zwingend zur Erfüllung einer gesetzlichen Aufgabe erforderlich ist, unerheblich, ob die mit den fraglichen Datenbearbeitungen befassten Personen einer (gesetzlich vorgesehenen) Schweigepflicht oder einem Amtsgeheimnis unterliegen. Denn diese Aspekte stehen mit den Anforderungen des Verhältnismässigkeitsprinzips nicht im Zusammenhang; dieses ist vielmehr unabhängig von derartigen Pflichten zu beachten. Insbesondere kann aus diesen Pflichten

nicht abgeleitet werden, dass einer solchen Schweigepflicht unterstehende Personen eine Art erleichterter Zugang zu Daten haben dürften.²⁹

Weiter wird man verlangen müssen, dass die gesetzliche Aufgabe hinreichend bestimmt umschrieben ist, kann doch nur auf dieser Grundlage eruiert werden, ob die entsprechende Datenbearbeitung für ihre Erfüllung unentbehrlich ist.³⁰ Auf Bundesebene ist zusätzlich ein Gesetz im formellen Sinn notwendig (Art. 17 Abs. 2 lit. a DSG); in den Kantonen ist diese Anforderung nicht durchgängig so formuliert. Gute Gründe – insbesondere das Gesetzmässigkeitsprinzip – sprechen aber dafür, dass grundsätzlich ein Gesetz auch auf kantonaler Ebene ein Gesetz im formellen Sinn notwendig ist.

Fraglich könnte in diesem Zusammenhang noch sein, ob die Datenbearbeitung nur im Einzelfall erfolgen darf, womit eine systematische und regelmässige Datenbearbeitung nicht im Einklang stünde. Dieser Ansatz wird im Zusammenhang mit Art. 17 Abs. 2 DSG mit dem Argument vertreten, diese Bestimmung sehe die in Art. 17 Abs. 2 lit. a-c DSG genannten Konstellationen ausdrücklich als „Ausnahmekonstellationen“ vor.³¹ Dieses Argument greift jedoch auf kantonaler Ebene nicht zwingend, da hier zumindest teilweise die Verankerung der Bearbeitung in einer gesetzlichen Grundlage „gleichberechtigt“ neben Surrogaten einer solchen steht. Immerhin sei aber darauf hingewiesen, dass sich aus den allgemeinen Grundsätzen des Gesetzmässigkeitsprinzips ergeben dürfte, dass bei Bearbeitungen besonders schützenswerter Personendaten in einem gewissen Umfang und einer gewissen Regelmässigkeit die Verankerung der betreffenden gesetzlichen Aufgabe in einem Gesetz im formellen Sinn notwendig erscheint, geht es hier doch um wichtige rechtsetzende Bestimmungen sowie um Massnahmen, mit denen ein gewisses Risiko für Persönlichkeitsverletzungen verbunden ist.

Ob und inwieweit den skizzierten Anforderungen in Bezug auf eine bestimmte Datenbearbeitung und ihre Ausgestaltung im Einzelnen Genüge getan ist, kann selbstredend nur auf der Grundlage einer genauen Analyse der Art und des Umfangs der in Frage stehenden Datenbearbeitung beantwortet werden. Regelmässig problematisch dürfte in diesem Zusammenhang weniger die grundsätzliche Zulässigkeit der Datenbearbeitung, denn ihre konkrete Ausgestaltung, etwa in Bezug auf die Reichweite der Zugriffsberechtigten, den Umfang der gespeicherten Daten oder ihre Aufbewahrungsdauer, sein. Denn häufig wird die Bearbeitung besonders schützenswerter Personendaten grundsätzlich für die Wahrnehmung einer gesetzlich vorgesehenen Aufgabe notwendig sein, so z.B., wenn es um die Frage geht, ob eine Person sozialhilfeberechtigt

²⁹ Zumindest missverständlich jedoch BGE 133 V 359. Vgl. zu dieser Problematik im Zusammenhang mit Krankenversicherungsdaten UTTINGER, HAVE 2007, 253 ff.

³⁰ In diese Richtung auch wohl die bundesgerichtliche Rechtsprechung in Bezug auf Art. 17 Abs. 2 lit. a DSG, vgl. BGE 124 III 170 E. 4a. Ausdrücklich auch z.B. JÖHRI/STUDER, in: Mauer-Lambrou/Vogt, BK Datenschutzgesetz, Art. 17, Rn. 47.

³¹ JÖHRI, in: Rosenthal/Jöhri, Handkommentar DSG, Art. 17, Rn. 76; JÖHRI/STUDER, in: Mauer-Lambrou/Vogt, BK Datenschutzgesetz, Art. 17, Rn. 47; so auch EDÖB, Empfehlung betreffend Drogen- und Alkoholtastes bei den SBB v. 25.5.2007, Ziff. II.6.

ist oder in Bezug auf sie fürsorgliche Massnahmen getroffen werden dürfen oder gar müssen.

Auch wenn damit die grundsätzliche Zulässigkeit der Datenbearbeitung häufig mit guten Gründen zu bejahen sein kann, ist nach dem Gesagten auch bei ihrer Ausgestaltung im Einzelnen danach zu fragen, ob sie tatsächlich – in der vorgesehenen Form und in dem vorgesehenen Ausmass – für die Erfüllung einer gesetzlichen Aufgabe nicht nur sachdienlich, sondern geradezu unverzichtbar ist. Daher reichen Erwägungen der Verwaltungseffizienz bzw. der Arbeitserleichterung nicht aus, um eine bestimmte Art der Datenbearbeitung zu begründen, sofern sie nicht zu einer Verunmöglichung der Wahrnehmung der gesetzlichen Aufgabe führen, was die grosse Ausnahme darstellen dürfte. Dieser Grundsatz impliziert auch, dass sich die konkrete Organisation der Erfüllung der gesetzlichen Aufgabe in der und durch die Verwaltung an den erörterten datenschutzrechtlichen Anforderungen zu orientieren hat (und nicht umgekehrt).

Diese Grundsätze können am Beispiel der gerade bei Informationssystemen häufig in Frage stehenden Reichweite des Zugriffs zu besonders schützenswerten Personendaten etwas illustriert werden: Ausgangspunkt ist hier, dass der Zugang zu den jeweiligen Personendaten der Betroffenen nur soweit gewährt werden darf, wie dies zur Erfüllung der jeweiligen gesetzlichen Aufgaben zwingend erforderlich ist, so dass nur denjenigen Personen bzw. Stellen eine Zugangsberechtigung zu gewähren ist, die tatsächlich in Bezug auf die betroffene Person die gesetzlichen Aufgaben wahrnehmen (in dem sie diese z.B. betreut, ihre Sozialhilfebedürftigkeit abzuklären hat oder administrative Unterstützungsarbeit leistet). Im Übrigen impliziert die „zwingende“ Erforderlichkeit auch, dass der Zugang soweit wie möglich – in Bezug auf die Zahl der zugangsberechtigten Personen – einzuschränken ist. Auf dieser Grundlage können folgende Leitlinien für eine rechtmässige Ausgestaltung des Zugangs formuliert werden:

- Zugangsberechtigt müssen bzw. dürfen jedenfalls die für die „Betreuung“ der jeweiligen Personen zuständigen Mitarbeitenden bzw. Stellen der Ämter sein.
- Im Hinblick auf eine effektive (nicht nur effiziente) Wahrnehmung der gesetzlichen Aufgaben kann dies in der Regel nicht nur eine Person bzw. eine Stelle sein, sondern geboten und zulässig ist auch der Zugang zu den Dossiers für mehrere Personen. Nur auf diese Weise kann dem Umstand Rechnung getragen werden, dass es in den Ämtern Teilzeitbeschäftigte geben kann und die Betreuung im Übrigen auch im Krankheitsfall oder bei einem Urlaub sichergestellt werden muss.
- Allerdings ist die Zahl der Zugangsberechtigten vor dem Hintergrund der geforderten „zwingenden“ Erforderlichkeit der Datenbearbeitung möglichst gering zu halten. Insofern ist jeweils näher zu prüfen, ob in den betroffenen Ämtern bzw. Sektionen zwingend immer allen Mitarbeitenden

ein Zugriffsrecht gewährt werden muss, was letztlich von der Grösse der einzelnen Sektionen und der von den einzelnen Mitarbeitenden wahrgenommenen Aufgaben abhängt.

- Auch kann es bei bestimmten Aufgaben (z.B. in den Sozialämtern) notwendig sein, dass ein sog. „Pikettdienst“ – der für Notfälle zuständig ist – Zugang zu allen Dossiers hat, da nur auf diese Weise ausserhalb der ordentlichen Arbeitszeiten Notfälle betreut werden können. Allerdings würde sich hier wohl eine zeitliche Beschränkung aufdrängen, trägt diese Erwägung doch nur während der Wahrnehmung des Pikettdienstes.
- Nicht ersichtlich ist, dass es zur Erfüllung der gesetzlichen Aufgaben zwingend notwendig ist, dass allgemein zentrale Dienste (z.B. solche der Postverteilung) Zugang zu den Dossiers haben.
- Soweit Teile eines Amtes mit buchhalterischen und / oder „finanziellen“ Aufgaben (Revisionen, Berechnungen finanzieller Beiträge, o.ä.) betraut sind, erscheint es zumindest nicht grundsätzlich notwendig, dass diese Stellen als solche umfassend und spontan Zugang zu den Dossiers haben, da jedenfalls einige Aufgaben wohl auch ohne die Kenntnis des vollständigen Dossiers bzw. Moduls wahrgenommen werden können.
- Ganz allgemein vermag allein eine gewisse (administrative) Vereinfachung der Tätigkeit der Behörde eine Zugangsberechtigung bzw. deren Erweiterung nicht zu begründen, würde damit doch dem Erfordernis der „zwingenden“ Erforderlichkeit der Datenbearbeitung für die Wahrnehmung der gesetzlichen Aufgabe nicht Rechnung getragen. Daher ist ggf. – statt eines generalisierten Zugangs einer bestimmten Sektion oder eines Teils eines Amtes zu einem Dossier – eine einzelfallweise Übermittlung von Daten auf Anfrage oder auf Initiative eines Zugangsberechtigten in Betracht zu ziehen, die sich im Übrigen ggf. auf die konkret notwendigen Angaben beschränken kann (z.B. gewisse Angaben über die finanzielle Situation einer Person, unter Aussparung sonstiger, in dem Dossier möglicherweise enthaltener Informationen).
- Schliesslich ist generell auch immer danach zu fragen, ob nicht eingeschränkte Zugangsrechte (sei dies inhaltlich oder / und zeitlich) oder Zugänge bzw. bestimmte Datenübermittlungen im Einzelfall für die Wahrnehmung der gesetzlichen Aufgabe ausreichend sein könnten.

IV. Schlussbemerkung

Insgesamt sind nach dem Gesagten der Bearbeitung besonders schützenswerter Personendaten durch öffentliche Organe im Falle einer fehlenden gesetzlichen Grundlage gerade für diese Bearbeitung letztlich enge Grenzen gesetzt. Auch konnten deren Umrisse etwas präzisierter werden; nichtsdestotrotz ist nicht zu verkennen, dass die Frage, unter welchen

Voraussetzung eine bestimmte Bearbeitung besonders schützenswerter Personendaten zur Erfüllung des gesetzlich formulierten Zwecks nun wirklich „zwingend“ erforderlich ist, nicht immer einfach zu entscheiden ist und auch eine gewisse Abwägung impliziert.

Da die Bearbeitung besonders schützenswerter Personendaten aber für die Betroffenen in der Regel einen weitgehenden Eingriff in ihre Persönlichkeitsrechte impliziert, ist nach der hier vertretenen Ansicht eine gesetzliche Verankerung, zumindest bei Informationssystemen, grundsätzlich sehr sachdienlich, wenn nicht gar verfassungsrechtlich gefordert.³² Angesichts der nach wie vor bestehenden Unschärfe des Kriteriums der zwingenden Erforderlichkeit erscheint es nämlich vor dem Hintergrund des Gesetzmässigkeitsprinzips bedenklich, die hier zu treffenden Entscheidungen der Verwaltung zu überantworten. Eine klare gesetzliche Regelung, die auf die genauen Bearbeitungszwecke Bezug nimmt, den Umfang der Datenbearbeitung, die an der Datenbearbeitung Beteiligten, die Kategorien der bearbeiteten Daten sowie die Dauer der Datenaufbewahrung bzw. die Voraussetzungen der Löschung der Daten definiert, erschiene hier sowohl in Bezug auf die Rechte der Betroffenen und eine gewisse Transparenz als auch die Wahrung der Prärogative des Gesetzgebers zumindest sinnvoll, wenn nicht gar verfassungsrechtlich geboten.

Im Übrigen ist nicht zu verkennen, dass mit der Erfüllung datenschutzrechtlicher Anforderungen Effizienzverluste bzw. ein höherer Aufwand für die Verwaltung einhergehen kann und häufig auch wird. So wird Datenschutz denn auch häufig als „Effizienzhindernis“ für die Wahrnehmung bestimmter (öffentlicher) Aufgaben angesehen. Diese Feststellung ist durchaus im Grundsatz zutreffend, wäre es doch für die Behörden am effizientesten, wenn möglichst viele Daten der Bürger und Bürgerinnen bei ihnen vorhanden und möglichst schrankenlos zugänglich wären und ausgetauscht werden könnten. In einem Rechtsstaat darf jedoch Effizienz grundsätzlich kein Kriterium dafür sein, als wesentlich eingestufte Errungenschaften eben dieses Rechtsstaats „ausser Kraft zu setzen“. Vielmehr ist der Rechtsstaat an sich teilweise (zumindest zunächst) ineffizient; man denke etwa – über die in diesem Beitrag angesprochenen Fragen hinaus – an die Vorgaben für ein faires Verfahren oder an die durch die Polizei zu beachtenden Vorschriften. Nur am Rande sei in diesem Zusammenhang bemerkt, dass der zunächst und zumindest teilweise nur anscheinend bestehende „Gewinn“ an Effizienz durch Abstriche bei der Beachtung rechtsstaatlicher Grundsätze sich durchaus zumindest mittelfristig in das Gegenteil verkehren kann, „profitiert“ der Staat doch von der Akzeptanz, die einem demokratischen Rechtsstaat seitens der Bürgerinnen

³² Wie bereits erwähnt (oben II.), sind die allgemeinen datenschutzrechtlichen Grundsätze (vgl. Art. 4 DSG, Art. 5 KDSG) letztlich Ausprägungen bzw. Konkretisierungen der bereits in der Verfassung (Art. 13 Abs. 2 BV) und der EMRK (Art. 8 EMRK) enthaltenen Vorgaben, vgl. in Bezug auf die gesetzliche Grundlage auch BGE 122 I 360, E. 5.b)dd).

und Bürger entgegen gebracht wird. Insofern lohnt es sich, die Anstrengungen und den Aufwand auf sich zu nehmen, um einen über jeden (rechtlichen) Zweifel erhabenen Standard an Datenschutz und damit an Grundrechtsschutz zu gewährleisten, zumal es die erörterten Garantien durchaus erlauben, die in Frage stehenden öffentlichen Interessen zu verfolgen.

Literatur

- BELSER, EVA MARIA/EPINEY, ASTRID/WALDMANN, BERNHARD: Datenschutzrecht. Grundlagen und öffentliches Recht, Bern 2011 (zitiert: VERFASSTER, in: Belser/Epiney/Waldmann, Datenschutzrecht).
- EPINEY, ASTRID/HOFSTÖTTER, BERNHARD/MEIER, ANNEKATHRIN/THEUERKAUF, SARAH: Schweizerisches Datenschutzrecht vor europa- und völkerrechtlichen Herausforderungen. Zur rechtlichen Tragweite der europa- und völkerrechtlichen Vorgaben und ihren Implikationen für die Schweiz, Zürich 2007.
- FASNACHT, TOBIAS: Die Revision der Datenschutzkonvention des Europarates. Implikationen für die Schweiz, in: Astrid Epiney/Tobias Fasnacht (Hrsg.), Schweizerisches Jahrbuch für Europarecht (SJER) 2011/2012, Zürich/Bern 2012, 329 ff.
- HÄNER, ISABELLE: Die Einwilligung der betroffenen Person als Surrogat der gesetzlichen Grundlage bei individuell-konkreten Staatshandlungen, ZBl. 2002, 57 ff.
- MAURER-LAMBROU, URS/VOGT, NEDIM PETER (Hrsg.): Datenschutzgesetz, Basler Kommentar, 2. Aufl., Basel 2006 (zitiert: VERFASSTER, in: Mauer-Lambrou/Vogt, BK Datenschutzgesetz).
- MEIER, PHILIPPE: Protection des données, Fondements, principes généraux et droit privé, Bern 2011
- ROSENTHAL, DAVID/JÖHRI, YVONNE: Handkommentar zum Datenschutzgesetz, sowie weiteren, ausgewählten Bestimmungen, Zürich 2008 (zitiert: VERFASSTER, in: Rosenthal/Jöhri, Handkommentar DSG).
- SCHWEIZER, ALEX: Data Mining, Data Warehouse, Zürich 1999.
- STEINAUER, PAUL-HENRI: La jurisprudence de la Commission fédérale de la protection des données et de la transparence au sujet du traitement de données par des personnes privées, ZBl. 2007, 354 ff.
- DE TERWANGNE, CÉCILE: La modernisation de la Convention 108 du Conseil de l'Europe, in: Astrid Epiney/Tobias Fasnacht (Hrsg.), Die Entwicklung der europarechtlichen Vorgaben im Bereich des Datenschutzes und Implikationen für die Schweiz / Le développement du droit européen en matière de protection des données et ses implications pour la Suisse, Zürich 2012, 23 ff.

UTTINGER, URSULA: Datenschutz in der Krankenversicherung, insbesondere im vertrauensärztlichen Dienst, HAVE 2007, 253 ff.

WEBER, ROLF H.: Datenschutzrecht vor neuen Herausforderungen. Marketing – E-Commerce – Virtuelle Bank – Sachdaten, Zürich 2000

WERMELINGER, AMÉDÉO/SCHWERI, DANIEL: Teilrevision des Eidgenössischen Datenschutzrechts – Es nützt nicht viel, schadet es etwas?, Jusletter v. 3.3.2008.